

ISC2

Exam Questions SSCP

System Security Certified Practitioner (SSCP)



NEW QUESTION 1

- (Topic 1)

Which of the following pairings uses technology to enforce access control policies?

- A. Preventive/Administrative
- B. Preventive/Technical
- C. Preventive/Physical
- D. Detective/Administrative

Answer: B

Explanation:

The preventive/technical pairing uses technology to enforce access control policies.

TECHNICAL CONTROLS

Technical security involves the use of safeguards incorporated in computer hardware, operations or applications software, communications hardware and software, and related devices. Technical controls are sometimes referred to as logical controls.

Preventive Technical Controls

Preventive technical controls are used to prevent unauthorized personnel or programs from gaining remote access to computing resources. Examples of these controls include:

Access control software. Antivirus software. Library control systems. Passwords.

Smart cards. Encryption.

Dial-up access control and callback systems.

Preventive Physical Controls

Preventive physical controls are employed to prevent unauthorized personnel from entering computing facilities (i.e., locations housing computing resources, supporting utilities, computer hard copy, and input data media) and to help protect against natural disasters. Examples of these controls include:

Backup files and documentation. Fences.

Security guards. Badge systems. Double door systems. Locks and keys. Backup power.

Biometric access controls. Site selection.

Fire extinguishers.

Preventive Administrative Controls

Preventive administrative controls are personnel-oriented techniques for controlling people's behavior to ensure the confidentiality, integrity, and availability of computing data and programs. Examples of preventive administrative controls include:

Security awareness and technical training. Separation of duties.

Procedures for recruiting and terminating employees. Security policies and procedures.

Supervision.

Disaster recovery, contingency, and emergency plans. User registration for computer access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 2

- (Topic 1)

Which type of password token involves time synchronization?

- A. Static password tokens
- B. Synchronous dynamic password tokens
- C. Asynchronous dynamic password tokens
- D. Challenge-response tokens

Answer: B

Explanation:

Synchronous dynamic password tokens generate a new unique password value at fixed time intervals, so the server and token need to be synchronized for the password to be accepted.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

Also check out: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw- Hill/Osborne, 2002, chapter 4: Access Control (page 136).

NEW QUESTION 3

- (Topic 1)

Which is the last line of defense in a physical security sense?

- A. people
- B. interior barriers
- C. exterior barriers
- D. perimeter barriers

Answer: A

Explanation:

"Ultimately, people are the last line of defense for your company's assets" (Pastore & Dulaney, 2006, p. 529).

Pastore, M. and Dulaney, E. (2006). CompTIA Security+ study guide: Exam SY0-101. Indianapolis, IN: Sybex.

NEW QUESTION 4

- (Topic 1)

Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is not a component that achieves this type of security?

- A. Administrative control mechanisms
- B. Integrity control mechanisms
- C. Technical control mechanisms
- D. Physical control mechanisms

Answer: B

Explanation:

Integrity Controls Mechanisms are not part of physical security. All of the other detractors were correct this one was the wrong one that does not belong to Physical Security. Below you have more details extracted from the SearchSecurity web site: Information security depends on the security and management of the physical space in which computer systems operate. Domain 9 of the CISSP exam's Common Body of Knowledge addresses the challenges of securing the physical space, its systems and the people who work within it by use of administrative, technical and physical controls. The following QUESTION NO: s are covered:

Facilities management: The administrative processes that govern the maintenance and protection of the physical operations space, from site selection through emergency response.

Risks, issues and protection strategies: Risk identification and the selection of security protection components.

Perimeter security: Typical physical protection controls.

Facilities management

Facilities management is a complex component of corporate security that ranges from the planning of a secure physical site to the management of the physical information system environment. Facilities management responsibilities include site selection and physical security planning (i.e. facility construction, design and layout, fire and water damage protection, antitheft mechanisms, intrusion detection and security procedures.) Protections must extend to both people and assets. The necessary level of protection depends on the value of the assets and data. CISSP® candidates must learn the concept of critical-path analysis as a means of determining a component's business function criticality relative to the cost of operation and replacement. Furthermore, students need to gain an understanding of the optimal location and physical attributes of a secure facility. Among the QUESTION NO: s covered in this domain are site inspection, location, accessibility and obscurity, considering the area crime rate, and the likelihood of natural hazards such as floods or earthquakes.

This domain also covers the quality of construction material, such as its protective qualities and load capabilities, as well as how to lay out the structure to minimize risk of forcible entry and accidental damage. Regulatory compliance is also touched on, as is preferred proximity to civil protection services, such as fire and police stations. Attention is given to computer and equipment rooms, including their location, configuration (entrance/egress requirements) and their proximity to wiring distribution centers at the site.

Physical risks, issues and protection strategies

An overview of physical security risks includes risk of theft, service interruption, physical damage, compromised system integrity and unauthorized disclosure of information. Interruptions to business can manifest due to loss of power, services, telecommunications connectivity and water supply. These can also seriously compromise electronic security monitoring alarm/response devices. Backup options are also covered in this domain, as is a strategy for quantifying the risk exposure by simple formula.

Investment in preventive security can be costly. Appropriate redundancy of people skills, systems and infrastructure must be based on the criticality of the data and assets to be preserved. Therefore a strategy is presented that helps determine the selection of cost appropriate controls. Among the QUESTION NO: s covered in this domain are regulatory and legal requirements, common standard security protections such as locks and fences, and the importance of establishing service level agreements for maintenance and disaster support. Rounding out the optimization approach are simple calculations for determining mean time between failure and mean time to repair (used to estimate average equipment life expectancy) ?? essential for estimating the cost/benefit of purchasing and maintaining redundant equipment.

As the lifeblood of computer systems, special attention is placed on adequacy, quality and protection of power supplies. CISSP candidates need to understand power supply concepts and terminology, including those for quality (i.e. transient noise vs. clean power); types of interference (EMI and RFI); and types of interruptions such as power excess by spikes and surges, power loss by fault or blackout, and power degradation from sags and brownouts. A simple formula is presented for determining the total cost per hour for backup power. Proving power reliability through testing is recommended and the advantages of three power protection approaches are discussed (standby UPS, power line conditioners and backup sources) including minimum requirements for primary and alternate power provided.

Environmental controls are explored in this domain, including the value of positive pressure water drains and climate monitoring devices used to control temperature, humidity and reduce static electricity. Optimal temperatures and humidity settings are provided.

Recommendations include strict procedures during emergencies, preventing typical risks (such as blocked fans), and the use of antistatic armbands and hygrometers. Positive pressurization for proper ventilation and monitoring for air born contaminants is stressed.

The pros and cons of several detection response systems are deeply explored in this domain. The concept of combustion, the classes of fire and fire extinguisher ratings are detailed. Mechanisms behind smoke-activated, heat-activated and flame-activated devices and Automatic Dial-up alarms are covered, along with their advantages, costs and shortcomings. Types of fire sources are distinguished and the effectiveness of fire suppression methods for each is included. For instance, Halon and its approved replacements are covered, as are the advantages and the inherent risks to equipment of the use of water sprinklers.

Administrative controls

The physical security domain also deals with administrative controls applied to physical sites and assets. The need for skilled personnel, knowledge sharing between them, separation of duties, and appropriate oversight in the care and maintenance of equipment and environments is stressed. A list of management duties including hiring checks, employee maintenance activities and recommended termination procedures is offered. Emergency measures include accountability for evacuation and system shutdown procedures, integration with disaster and business continuity plans, assuring documented procedures are easily available during different types of emergencies, the scheduling of periodic equipment testing, administrative reviews of documentation, procedures and recovery plans, responsibilities delegation, and personnel training and drills.

Perimeter security

Domain nine also covers the devices and techniques used to control access to a space. These include access control devices, surveillance monitoring, intrusion detection and corrective actions. Specifications are provided for optimal external boundary protection, including fence heights and placement, and lighting placement and types. Selection of door types and lock characteristics are covered. Surveillance methods and intrusion-detection methods are explained, including the use of video monitoring, guards, dogs, proximity detection systems, photoelectric/photometric systems, wave pattern devices, passive infrared systems, and sound and motion detectors, and current flow sensitivity devices that specifically address computer theft. Room lock types ?? both preset and cipher locks (and their variations) -- device locks, such as portable laptop locks, lockable server bays, switch control locks and slot locks, port controls, peripheral switch controls and cable trap locks are also covered. Personal access control methods used to identify authorized users for site entry are covered at length, noting social engineering risks such as piggybacking. Wireless proximity devices, both user access and system sensing readers are covered (i.e. transponder based, passive devices and field powered devices) in this domain.

Now that you've been introduced to the key concepts of Domain 9, watch the Domain 9, Physical Security video

Return to the CISSP Essentials Security School main page

See all SearchSecurity.com's resources on CISSP certification training Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2001, Page 280.

NEW QUESTION 5

- (Topic 1)

Crime Prevention Through Environmental Design (CPTED) is a discipline that:

- A. Outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior.
- B. Outlines how the proper design of the logical environment can reduce crime by directly affecting human behavior.

- C. Outlines how the proper design of the detective control environment can reduce crime by directly affecting human behavior.
- D. Outlines how the proper design of the administrative control environment can reduce crime by directly affecting human behavior.

Answer: A

Explanation:

Crime Prevention Through Environmental Design (CPTED) is a discipline that outlines how the proper design of a physical environment can reduce crime by directly affecting human behavior. It provides guidance about lost and crime prevention through proper facility construction and environmental components and procedures.

CPTED concepts were developed in the 1960s. They have been expanded upon and have matured as our environments and crime types have evolved. CPTED has been used not just to develop corporate physical security programs, but also for large-scale activities such as development of neighborhoods, towns, and cities. It addresses landscaping, entrances, facility and neighborhood layouts, lighting, road placement, and traffic circulation patterns. It looks at microenvironments, such as offices and rest-rooms, and macroenvironments, like campuses and cities.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 435). McGraw- Hill. Kindle Edition.

and

CPTED Guide Book

NEW QUESTION 6

- (Topic 1)

Which of the following is most affected by denial-of-service (DOS) attacks?

- A. Confidentiality
- B. Integrity
- C. Accountability
- D. Availability

Answer: D

Explanation:

Denial of service attacks obviously affect availability of targeted systems. Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 61).

NEW QUESTION 7

- (Topic 1)

In the Bell-LaPadula model, the Star-property is also called:

- A. The simple security property
- B. The confidentiality property
- C. The confinement property
- D. The tranquility property

Answer: B

Explanation:

The Bell-LaPadula model focuses on data confidentiality and access to classified information, in contrast to the Biba Integrity Model which describes rules for the protection of data integrity.

In this formal model, the entities in an information system are divided into subjects and objects.

The notion of a "secure state" is defined, and it is proven that each state transition preserves security by moving from secure state to secure state, thereby proving that the system satisfies the security objectives of the model.

The Bell-LaPadula model is built on the concept of a state machine with a set of allowable states in a system. The transition from one state to another state is defined by transition functions.

A system state is defined to be "secure" if the only permitted access modes of subjects to objects are in accordance with a security policy.

To determine whether a specific access mode is allowed, the clearance of a subject is compared to the classification of the object (more precisely, to the combination of classification and set of compartments, making up the security level) to determine if the subject is authorized for the specific access mode.

The clearance/classification scheme is expressed in terms of a lattice. The model defines two mandatory access control (MAC) rules and one discretionary access control (DAC) rule with three security properties:

The Simple Security Property - a subject at a given security level may not read an object at a higher security level (no read-up).

The property (read "star"-property) - a subject at a given security level must not write to any object at a lower security level (no write-down). The property is also known as the Confinement property.

The Discretionary Security Property - use an access control matrix to specify the discretionary access control.

The transfer of information from a high-sensitivity document to a lower-sensitivity document may happen in the Bell-LaPadula model via the concept of trusted subjects. Trusted Subjects are not restricted by the property. Untrusted subjects are.

Trusted Subjects must be shown to be trustworthy with regard to the security policy. This security model is directed toward access control and is characterized by the phrase: "no read up, no write down." Compare the Biba model, the Clark-Wilson model and the Chinese Wall.

With Bell-LaPadula, users can create content only at or above their own security level (i.e. secret researchers can create secret or top-secret files but may not create public files; no write-down). Conversely, users can view content only at or below their own security level (i.e. secret researchers can view public or secret files, but may not view top-secret files; no read-up).

Strong Property

The Strong Property is an alternative to the Property in which subjects may write to objects with only a matching security level. Thus, the write-up operation permitted in the usual Property is not present, only a write-to-same level operation. The Strong Property is usually discussed in the context of multilevel database management systems and is motivated by integrity concerns.

Tranquility principle

The tranquility principle of the Bell-LaPadula model states that the classification of a subject or object does not change while it is being referenced. There are two forms to the tranquility principle: the "principle of strong tranquility" states that security levels do not change during the normal operation of the system and the "principle of weak tranquility" states that security levels do not change in a way that violates the rules of a given security policy.

Another interpretation of the tranquility principles is that they both apply only to the period of time during which an operation involving an object or subject is occurring. That is, the strong tranquility principle means that an object's security level/label will not change during an operation (such as read or write); the weak tranquility principle means that an object's security level/label may change in a way that does not violate the security policy during an operation.

Reference(s) used for this question: http://en.wikipedia.org/wiki/Biba_Model

http://en.wikipedia.org/wiki/Mandatory_access_control http://en.wikipedia.org/wiki/Discretionary_access_control http://en.wikipedia.org/wiki/Clark-Wilson_model

http://en.wikipedia.org/wiki/Brewer_and_Nash_model

NEW QUESTION 8

- (Topic 1)

In which of the following model are Subjects and Objects identified and the permissions applied to each subject/object combination are specified. Such a model can be used to quickly summarize what permissions a subject has for various system objects.

- A. Access Control Matrix model
- B. Take-Grant model
- C. Bell-LaPadula model
- D. Biba model

Answer: A

Explanation:

An access control matrix is a table of subjects and objects indicating what actions individual subjects can take upon individual objects. Matrices are data structures that programmers implement as table lookups that will be used and enforced by the operating system.

This type of access control is usually an attribute of DAC models. The access rights can be assigned directly to the subjects (capabilities) or to the objects (ACLs). Capability Table

A capability table specifies the access rights a certain subject possesses pertaining to specific objects. A capability table is different from an ACL because the subject is bound to the capability table, whereas the object is bound to the ACL.

Access control lists (ACLs)

ACLs are used in several operating systems, applications, and router configurations. They are lists of subjects that are authorized to access a specific object, and they define what level of authorization is granted. Authorization can be specific to an individual, group, or role. ACLs map values from the access control matrix to the object.

Whereas a capability corresponds to a row in the access control matrix, the ACL corresponds to a column of the matrix.

NOTE: Ensure you are familiar with the terms Capability and ACLs for the purpose of the exam.

Resource(s) used for this question:

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition (Kindle Locations 5264-5267). McGraw-Hill. Kindle Edition.

or

Harris, Shon (2012-10-25). CISSP All-in-One Exam Guide, 6th Edition, Page 229 and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1923-1925). Auerbach Publications. Kindle Edition.

NEW QUESTION 9

- (Topic 1)

Controls to keep password sniffing attacks from compromising computer systems include which of the following?

- A. static and recurring passwords.
- B. encryption and recurring passwords.
- C. one-time passwords and encryption.
- D. static and one-time passwords.

Answer: C

Explanation:

To minimize the chance of passwords being captured one-time passwords would prevent a password sniffing attack because once used it is no longer valid. Encryption will also minimize these types of attacks.

The following answers are correct:

static and recurring passwords. This is incorrect because if there is no encryption then someone password sniffing would be able to capture the password much easier if it never changed.

encryption and recurring passwords. This is incorrect because while encryption helps, recurring passwords do nothing to minimize the risk of passwords being captured.

static and one-time passwords. This is incorrect because while one-time passwords will prevent these types of attacks, static passwords do nothing to minimize the risk of passwords being captured.

NEW QUESTION 10

- (Topic 1)

Which of the following access control models is based on sensitivity labels?

- A. Discretionary access control
- B. Mandatory access control
- C. Rule-based access control
- D. Role-based access control

Answer: B

Explanation:

Access decisions are made based on the clearance of the subject and the sensitivity label of the object.

Example: Eve has a "Secret" security clearance and is able to access the "Mugwump Missile Design Profile" because its sensitivity label is "Secret." She is denied access to the "Presidential Toilet Tissue Formula" because its sensitivity label is "Top Secret."

The other answers are not correct because:

Discretionary Access Control is incorrect because in DAC access to data is determined by the data owner. For example, Joe owns the "Secret Chili Recipe" and grants read access to Charles.

Role Based Access Control is incorrect because in RBAC access decisions are made based on the role held by the user. For example, Jane has the role "Auditor" and that role includes read permission on the "System Audit Log."

Rule Based Access Control is incorrect because it is a form of MAC. A good example would be a Firewall where rules are defined and apply to anyone connecting through the firewall.

References:

All in One third edition, page 164. Official ISC2 Guide page 187.

NEW QUESTION 10

- (Topic 1)

Which of the following can best eliminate dial-up access through a Remote Access Server as a hacking vector?

- A. Using a TACACS+ server.
- B. Installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall.
- C. Setting modem ring count to at least 5.
- D. Only attaching modems to non-networked hosts.

Answer: B

Explanation:

Containing the dial-up problem is conceptually easy: by installing the Remote Access Server outside the firewall and forcing legitimate users to authenticate to the firewall, any access to internal resources through the RAS can be filtered as would any other connection coming from the Internet.

The use of a TACACS+ Server by itself cannot eliminate hacking.

Setting a modem ring count to 5 may help in defeating war-dialing hackers who look for modem by dialing long series of numbers.

Attaching modems only to non-networked hosts is not practical and would not prevent these hosts from being hacked.

Source: STREBE, Matthew and PERKINS, Charles, Firewalls 24seven, Sybex 2000, Chapter 2: Hackers.

NEW QUESTION 11

- (Topic 1)

What does the Clark-Wilson security model focus on?

- A. Confidentiality
- B. Integrity
- C. Accountability
- D. Availability

Answer: B

Explanation:

The Clark-Wilson model addresses integrity. It incorporates mechanisms to enforce internal and external consistency, a separation of duty, and a mandatory integrity policy.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 5: Security Architectures and Models (page 205).

NEW QUESTION 12

- (Topic 1)

Which access control model provides upper and lower bounds of access capabilities for a subject?

- A. Role-based access control
- B. Lattice-based access control
- C. Biba access control
- D. Content-dependent access control

Answer: B

Explanation:

In the lattice model, users are assigned security clearances and the data is classified. Access decisions are made based on the clearance of the user and the classification of the object. Lattice-based access control is an essential ingredient of formal security models such as Bell-LaPadula, Biba, Chinese Wall, etc.

The bounds concept comes from the formal definition of a lattice as a "partially ordered set for which every pair of elements has a greatest lower bound and a least upper bound." To see the application, consider a file classified as "SECRET" and a user Joe with a security clearance of "TOP SECRET." Under Bell-LaPadula, Joe's "least upper bound" access to the file is "READ" and his least lower bound is "NO WRITE" (star property).

Role-based access control is incorrect. Under RBAC, the access is controlled by the permissions assigned to a role and the specific role assigned to the user.

Biba access control is incorrect. The Biba integrity model is based on a lattice structure but the context of the question disqualifies it as the best answer.

Content-dependent access control is incorrect. In content dependent access control, the actual content of the information determines access as enforced by the arbiter.

References:

CBK, pp. 324-325.

AIO3, pp. 291-293. See particularly Figure 5-19 on p. 293 for an illustration of bounds in action.

NEW QUESTION 17

- (Topic 1)

Which of the following statements pertaining to biometrics is FALSE?

- A. User can be authenticated based on behavior.
- B. User can be authenticated based on unique physical attributes.
- C. User can be authenticated by what he knows.
- D. A biometric system's accuracy is determined by its crossover error rate (CER).

Answer: C

Explanation:

As this is not a characteristic of Biometrics this is the right choice for this question. This is one of the three basic ways authentication can be performed and it is not related to Biometrics. Example of something you know would be a password or PIN for example.

Please make a note of the negative 'FALSE' within the question. This question may seem tricky to some of you but you would be amazed at how many people cannot deal with negative questions. There will be a few negative questions within the real exam, just like this one the keyword NOT or FALSE will be in Uppercase to clearly indicate that it is negative.

Biometrics verifies an individual's identity by analyzing a unique personal attribute or behavior, which is one of the most effective and accurate methods of

performing authentication (one to one matching) or identification (a one to many matching).

A biometric system scans an attribute or behavior of a person and compares it to a template store within an authentication server database, such template would be created in an earlier enrollment process. Because this system inspects the grooves of a person's fingerprint, the pattern of someone's retina, or the pitches of someone's voice, it has to be extremely sensitive.

The system must perform accurate and repeatable measurements of anatomical or physiological characteristics. This type of sensitivity can easily cause false positives or false negatives. The system must be calibrated so that these false positives and false negatives occur infrequently and the results are as accurate as possible.

There are two types of failures in biometric identification:

False Rejection also called False Rejection Rate (FRR) ?? The system fail to recognize a legitimate user. While it could be argued that this has the effect of keeping the protected area extra secure, it is an intolerable frustration to legitimate users who are refused access because the scanner does not recognize them. False Acceptance or False Acceptance Rate (FAR) ?? This is an erroneous recognition, either by confusing one user with another or by accepting an imposter as a legitimate user.

Physiological Examples:

Unique Physical Attributes:

Fingerprint (Most commonly accepted) Hand Geometry

Retina Scan (Most accurate but most intrusive) Iris Scan

Vascular Scan Behavioral Examples:

Repeated Actions Keystroke Dynamics

(Dwell time (the time a key is pressed) and Flight time (the time between "key up" and the next "key down").

Signature Dynamics

(Stroke and pressure points)

EXAM TIP:

Retina scan devices are the most accurate but also the most invasive biometrics system available today. The continuity of the retinal pattern throughout life and the difficulty in fooling such a device also make it a great long-term, high-security option. Unfortunately, the cost of the proprietary hardware as well the stigma of users thinking it is potentially harmful to the eye makes retinal scanning a bad fit for most situations.

Remember for the exam that fingerprints are the most commonly accepted type of biometrics system.

The other answers are incorrect:

'Users can be authenticated based on behavior.' is incorrect as this choice is TRUE as it pertains to BIOMETRICS.

Biometrics systems makes use of unique physical characteristics or behavior of users.

'User can be authenticated based on unique physical attributes.' is also incorrect as this choice is also TRUE as it pertains to BIOMETRICS. Biometrics systems makes use of unique physical characteristics or behavior of users.

'A biometric system's accuracy is determined by its crossover error rate (CER)' is also incorrect as this is TRUE as it also pertains to BIOMETRICS. The CER is the point at which the false rejection rates and the false acceptance rates are equal. The smaller the value of the CER, the more accurate the system.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25353-25356). Auerbach Publications. Kindle Edition.

and

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 25297-25303). Auerbach Publications. Kindle Edition.

NEW QUESTION 18

- (Topic 1)

Which of the following protocol was used by the INITIAL version of the Terminal Access Controller Access Control System TACACS for communication between clients and servers?

- A. TCP
- B. SSL
- C. UDP
- D. SSH

Answer: C

Explanation:

The original TACACS, developed in the early ARPANet days, had very limited functionality and used the UDP transport. In the early 1990s, the protocol was extended to include additional functionality and the transport changed to TCP.

TACACS is defined in RFC 1492, and uses (either TCP or UDP) port 49 by default. TACACS allows a client to accept a username and password and send a query to a TACACS authentication server, sometimes called a TACACS daemon or simply TACACSD. TACACSD uses TCP and usually runs on port 49. It would determine whether to accept or deny the authentication request and send a response back.

TACACS+

TACACS+ and RADIUS have generally replaced TACACS and XTACACS in more recently built or updated networks. TACACS+ is an entirely new protocol and is not compatible with TACACS or XTACACS. TACACS+ uses the Transmission Control Protocol (TCP) and RADIUS uses the User Datagram Protocol (UDP).

Since TCP is connection oriented

protocol, TACACS+ does not have to implement transmission control. RADIUS, however, does have to detect and correct transmission errors like packet loss, timeout etc. since it rides on UDP which is connectionless.

RADIUS encrypts only the users' password as it travels from the RADIUS client to RADIUS server. All other information such as the username, authorization, accounting are transmitted in clear text. Therefore it is vulnerable to different types of attacks. TACACS+ encrypts all the information mentioned above and therefore does not have the vulnerabilities present in the RADIUS protocol.

RADIUS and TACACS + are client/ server protocols, which means the server portion cannot send unsolicited commands to the client portion. The server portion can only speak when spoken to. Diameter is a peer-based protocol that allows either end to initiate communication. This functionality allows the Diameter server to send a message to the access server to request the user to provide another authentication credential if she is attempting to access a secure resource.

Reference(s) used for this question: <http://en.wikipedia.org/wiki/TACACS>

and

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 239). McGraw- Hill. Kindle Edition.

NEW QUESTION 23

- (Topic 1)

Which of the following is most relevant to determining the maximum effective cost of access control?

- A. the value of information that is protected
- B. management's perceptions regarding data importance

- C. budget planning related to base versus incremental spending.
- D. the cost to replace lost data

Answer: A

Explanation:

The cost of access control must be commensurate with the value of the information that is being protected.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 49.

NEW QUESTION 24

- (Topic 1)

Single Sign-on (SSO) is characterized by which of the following advantages?

- A. Convenience
- B. Convenience and centralized administration
- C. Convenience and centralized data administration
- D. Convenience and centralized network administration

Answer: B

Explanation:

Convenience -Using single sign-on users have to type their passwords only once when they first log in to access all the network resources; and Centralized Administration as some single sign-on systems are built around a unified server administration system. This allows a single administrator to add and delete accounts across the entire network from one user interface.

The following answers are incorrect:

Convenience - alone this is not the correct answer.

Centralized Data or Network Administration - these are thrown in to mislead the student. Neither are a benefit to SSO, as these specifically should not be allowed with just an SSO.

References: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, page 35.

TIPTON, Harold F. & HENRY, Kevin, Official (ISC)2 Guide to the CISSP CBK, 2007, page 180.

NEW QUESTION 29

- (Topic 1)

What is the PRIMARY use of a password?

- A. Allow access to files.
- B. Identify the user.
- C. Authenticate the user.
- D. Segregate various user's accesses.

Answer: C

Explanation:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 31

- (Topic 1)

Which of the following is used by RADIUS for communication between clients and servers?

- A. TCP
- B. SSL
- C. UDP
- D. SSH

Answer: C

Explanation:

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, Page 33.

NEW QUESTION 32

- (Topic 1)

Which of the following control pairings include: organizational policies and procedures, pre- employment background checks, strict hiring practices, employment agreements, employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks?

- A. Preventive/Administrative Pairing
- B. Preventive/Technical Pairing
- C. Preventive/Physical Pairing
- D. Detective/Administrative Pairing

Answer: A

Explanation:

The Answer: Preventive/Administrative Pairing: These mechanisms include organizational policies and procedures, pre-employment background checks, strict hiring practices, employment agreements, friendly and unfriendly employee termination procedures, vacation scheduling, labeling of sensitive materials, increased supervision, security awareness training, behavior awareness, and sign-up procedures to obtain access to information systems and networks.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 37

- (Topic 1)

Which of the following statements pertaining to biometrics is false?

- A. Increased system sensitivity can cause a higher false rejection rate
- B. The crossover error rate is the point at which false rejection rate equals the false acceptance rate.
- C. False acceptance rate is also known as Type II error.
- D. Biometrics are based on the Type 2 authentication mechanism.

Answer: D

Explanation:

Authentication is based on three factor types: type 1 is something you know, type 2 is something you have and type 3 is something you are. Biometrics are based on the Type 3 authentication mechanism.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 37).

NEW QUESTION 42

- (Topic 1)

Which of the following control pairing places emphasis on "soft" mechanisms that support the access control objectives?

- A. Preventive/Technical Pairing
- B. Preventive/Administrative Pairing
- C. Preventive/Physical Pairing
- D. Detective/Administrative Pairing

Answer: B

Explanation:

Soft Control is another way of referring to Administrative control.

Technical and Physical controls are NOT soft control, so any choice listing them was not the best answer.

Preventative/Technical is incorrect because although access control can be technical control, it is commonly not referred to as a "soft" control

Preventative/Administrative is correct because access controls are preventative in nature. it is always best to prevent a negative event, however there are times where controls might fail and you cannot prevent everything. Administrative controls are roles, responsibilities, policies, etc which are usually paper based. In the administrative category you would find audit, monitoring, and security awareness as well.

Preventative/Physical pairing is incorrect because Access controls with an emphasis on "soft" mechanisms conflict with the basic concept of physical controls, physical controls are usually tangible objects such as fences, gates, door locks, sensors, etc...

Detective/Administrative Pairing is incorrect because access control is a preventative control used to control access, not to detect violations to access.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.

NEW QUESTION 44

- (Topic 1)

Which of the following attacks could capture network user passwords?

- A. Data diddling
- B. Sniffing
- C. IP Spoofing
- D. Smurfing

Answer: B

Explanation:

A network sniffer captures a copy every packet that traverses the network segment the sniffer is connect to.

Sniffers are typically devices that can collect information from a communication medium, such as a network. These devices can range from specialized equipment to basic workstations with customized software.

A sniffer can collect information about most, if not all, attributes of the communication. The most common method of sniffing is to plug a sniffer into an existing network device like a hub or switch. A hub (which is designed to relay all traffic passing through it to all of its ports) will automatically begin sending all the traffic on that network segment to the sniffing device. On the other hand, a switch (which is designed to limit what traffic gets sent to which port) will have to be specially configured to send all traffic to the port where the sniffer is plugged in.

Another method for sniffing is to use a network tap??a device that literally splits a network transmission into two identical streams; one going to the original network destination and the other going to the sniffing device. Each of these methods has its advantages and disadvantages, including cost, feasibility, and the desire to maintain the secrecy of the sniffing activity.

The packets captured by sniffer are decoded and then displayed by the sniffer. Therfore, if the username/password are contained in a packet or packets traversing the segment the sniffer is connected to, it will capture and display that information (and any other information on that segment it can see).

Of course, if the information is encrypted via a VPN, SSL, TLS, or similar technology, the information is still captured and displayed, but it is in an unreadable format.

The following answers are incorrect:

Data diddling involves changing data before, as it is entered into a computer, or after it is extracted.

Spoofing is forging an address and inserting it into a packet to disguise the origin of the communication - or causing a system to respond to the wrong address.

Smurfing would refer to the smurf attack, where an attacker sends spoofed packets to the broadcast address on a gateway in order to cause a denial of service.

The following reference(s) were/was used to create this question: CISA Review manual 2014 Page number 321

Official ISC2 Guide to the CISSP 3rd edition Page Number 153

NEW QUESTION 46

- (Topic 1)

In biometric identification systems, at the beginning, it was soon apparent that truly positive identification could only be based on :

- A. sex of a person
- B. physical attributes of a person
- C. age of a person

D. voice of a person

Answer: B

Explanation:

Today implementation of fast, accurate reliable and user-acceptable biometric identification systems is already under way.
From: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 1, Page 7.

NEW QUESTION 51

- (Topic 1)

A central authority determines what subjects can have access to certain objects based on the organizational security policy is called:

- A. Mandatory Access Control
- B. Discretionary Access Control
- C. Non-Discretionary Access Control
- D. Rule-based Access control

Answer: C

Explanation:

A central authority determines what subjects can have access to certain objects based on the organizational security policy.

The key focal point of this question is the 'central authority' that determines access rights. Cecilia one of the quiz user has sent me feedback informing me that NIST defines MAC as:

"MAC Policy means that Access Control Policy Decisions are made by a CENTRAL

AUTHORITY. Which seems to indicate there could be two good answers to this question.

However if you read the NISTR document mentioned in the references below, it is also mentioned that: MAC is the most mentioned NDAC policy. So MAC is a form of NDAC policy.

Within the same document it is also mentioned: "In general, all access control policies other than DAC are grouped in the category of non- discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action."

Under NDAC you have two choices:

Rule Based Access control and Role Base Access Control

MAC is implemented using RULES which makes it fall under RBAC which is a form of NDAC. It is a subset of NDAC.

This question is representative of what you can expect on the real exam where you have more than once choice that seems to be right. However, you have to look closely if one of the choices would be higher level or if one of the choice falls under one of the other choice. In this case NDAC is a better choice because MAC is falling under NDAC through the use of Rule Based Access Control.

The following are incorrect answers: MANDATORY ACCESS CONTROL

In Mandatory Access Control the labels of the object and the clearance of the subject

determines access rights, not a central authority. Although a central authority (Better known as the Data Owner) assigns the label to the object, the system does the determination of access rights automatically by comparing the Object label with the Subject clearance. The subject clearance MUST dominate (be equal or higher) than the object being accessed.

The need for a MAC mechanism arises when the security policy of a system dictates that:

1. Protection decisions must not be decided by the object owner.
2. The system must enforce the protection decisions (i.e., the system enforces the security policy over the wishes or intentions of the object owner).

Usually a labeling mechanism and a set of interfaces are used to determine access based on the MAC policy; for example, a user who is running a process at the Secret classification should not be allowed to read a file with a label of Top Secret. This is known as the ??simple security rule,?? or ??no read up.?? Conversely, a user who is running a process with a label of Secret should not be allowed to write to a file with a label of Confidential. This rule is called the ??*-property?? (pronounced ??star property??) or ??no write down.?? The *-property is required to maintain system security in an automated environment.

DISCRETIONARY ACCESS CONTROL

In Discretionary Access Control the rights are determined by many different entities, each of the persons who have created files and they are the owner of that file, not one central authority.

DAC leaves a certain amount of access control to the discretion of the object's owner or anyone else who is authorized to control the object's access. For example, it is generally used to limit a user's access to a file; it is the owner of the file who controls other users' accesses to the file. Only those users specified by the owner may have some combination of read, write, execute, and other permissions to the file.

DAC policy tends to be very flexible and is widely used in the commercial and government sectors. However, DAC is known to be inherently weak for two reasons: First, granting read access is transitive; for example, when Ann grants Bob read access to a file, nothing stops Bob from copying the contents of Ann??s file to an object that Bob controls. Bob may now grant any other user access to the copy of Ann??s file without Ann??s knowledge.

Second, DAC policy is vulnerable to Trojan horse attacks. Because programs inherit the identity of the invoking user, Bob may, for example, write a program for Ann that, on the surface, performs some useful function, while at the same time destroys the contents of Ann??s files. When investigating the problem, the audit files would indicate that Ann destroyed her own files. Thus, formally, the drawbacks of DAC are as follows:

Discretionary Access Control (DAC) Information can be copied from one object to another; therefore, there is no real assurance on the flow of information in a system.

No restrictions apply to the usage of information when the user has received it.

The privileges for accessing objects are decided by the owner of the object, rather than through a system-wide policy that reflects the organization??s security requirements.

ACLs and owner/group/other access control mechanisms are by far the most common mechanism for implementing DAC policies. Other mechanisms, even though not designed with DAC in mind, may have the capabilities to implement a DAC policy.

RULE BASED ACCESS CONTROL

In Rule-based Access Control a central authority could in fact determine what subjects can have access when assigning the rules for access. However, the rules actually determine the access and so this is not the most correct answer.

RuBAC (as opposed to RBAC, role-based access control) allow users to access systems and information based on pre determined and configured rules. It is important to note that there is no commonly understood definition or formally defined standard for rule-based access control as there is for DAC, MAC, and RBAC.

??Rule-based access?? is a generic term applied to systems that allow some form of organization-defined rules, and therefore rule-based access control encompasses a broad range of systems. RuBAC may in fact be combined with other models, particularly RBAC or DAC. A RuBAC system intercepts every access request and compares the rules with the rights of the user to make an access decision. Most of the rule-based access control relies on a security label system, which dynamically composes a set of rules defined by a security policy. Security labels are attached to all objects, including files, directories, and devices.

Sometime roles to subjects (based on their attributes) are assigned as well. RuBAC meets the business needs as well as the technical needs of controlling service access. It allows business rules to be applied to access control??for example, customers who have overdue balances may be denied service access. As a mechanism for MAC, rules of RuBAC cannot be changed by users. The rules can be established by any attributes of a system related to the users such as domain, host, protocol, network, or IP addresses. For example, suppose that a user wants to access an object in another network on the other side of a router. The router employs RuBAC with the rule composed by the network addresses, domain, and protocol to decide whether or not the user can be granted access. If

employees change their roles within the organization, their existing authentication credentials remain in effect and do not need to be re configured. Using rules in conjunction with roles adds greater flexibility because rules can be applied to people as well as to devices. Rule-based access control can be combined with role-based access control, such that the role of a user is one of the attributes in rule setting. Some provisions of access control systems have rule-based policy engines in addition to a role-based policy engine and certain implemented dynamic policies [Des03]. For example, suppose that two of the primary types of software users are product engineers and quality engineers. Both groups usually have access to the same data, but they have different roles to perform in relation to the data and the application's function. In addition, individuals within each group have different job responsibilities that may be identified using several types of attributes such as developing programs and testing areas. Thus, the access decisions can be made in real time by a scripted policy that regulates the access between the groups of product engineers and quality engineers, and each individual within these groups. Rules can either replace or complement role-based access control. However, the creation of rules and security policies is also a complex process, so each organization will need to strike the appropriate balance.

References used for this question: <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf> and

AIO v3 p162-167 and OIG (2007) p.186-191

also

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33.

NEW QUESTION 52

- (Topic 1)

In addition to the accuracy of the biometric systems, there are other factors that must also be considered:

- A. These factors include the enrollment time and the throughput rate, but not acceptability.
- B. These factors do not include the enrollment time, the throughput rate, and acceptability.
- C. These factors include the enrollment time, the throughput rate, and acceptability.
- D. These factors include the enrollment time, but not the throughput rate, neither the acceptability.

Answer: C

Explanation:

In addition to the accuracy of the biometric systems, there are other factors that must also be considered.

These factors include the enrollment time, the throughput rate, and acceptability. Enrollment time is the time it takes to initially "register" with a system by providing samples

of the biometric characteristic to be evaluated. An acceptable enrollment time is around two minutes.

For example, in fingerprint systems, the actual fingerprint is stored and requires approximately 250kb per finger for a high quality image. This level of information is required for one-to-many searches in forensics applications on very large databases.

In finger-scan technology, a full fingerprint is not stored—the features extracted from this fingerprint are stored using a small template that requires approximately 500 to 1000 bytes of storage. The original fingerprint cannot be reconstructed from this template.

Updates of the enrollment information may be required because some biometric characteristics, such as voice and signature, may change with time.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37 & 38.

NEW QUESTION 53

- (Topic 1)

Which of the following questions is less likely to help in assessing physical access controls?

- A. Does management regularly review the list of persons with physical access to sensitive facilities?
- B. Is the operating system configured to prevent circumvention of the security software and application controls?
- C. Are keys or other access devices needed to enter the computer room and media library?
- D. Are visitors to sensitive areas signed in and escorted?

Answer: B

Explanation:

Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical access controls except for the one regarding operating system configuration, which is a logical access control.

Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self-Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

NEW QUESTION 57

- (Topic 1)

What is the primary role of smartcards in a PKI?

- A. Transparent renewal of user keys
- B. Easy distribution of the certificates between the users
- C. Fast hardware encryption of the raw data
- D. Tamper resistant, mobile storage and application of private keys of the users

Answer: D

Explanation:

Reference: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, 2001, McGraw-Hill/Osborne, page 139;
SNYDER, J., What is a SMART CARD?.

Wikipedia has a nice definition at: http://en.wikipedia.org/wiki/Tamper_resistance

Tamper-resistant microprocessors are used to store and process private or sensitive information, such as private keys or electronic money credit. To prevent an attacker from retrieving or modifying the information, the chips are designed so that the information is not accessible through external means and can be accessed only by the embedded software, which should contain the appropriate security measures.

Examples of tamper-resistant chips include all secure cryptoprocessors, such as the IBM 4758 and chips used in smartcards, as well as the Clipper chip. It has been argued that it is very difficult to make simple electronic devices secure against tampering, because numerous attacks are possible, including: physical attack of various forms (microprobing, drills, files, solvents, etc.) freezing the device applying out-of-spec voltages or power surges applying unusual clock signals

inducing software errors using radiation
measuring the precise time and power requirements of certain operations (see power analysis)
Tamper-resistant chips may be designed to zeroise their sensitive data (especially cryptographic keys) if they detect penetration of their security encapsulation or out-of-specification environmental parameters. A chip may even be rated for "cold zeroisation", the ability to zeroise itself even after its power supply has been crippled.
Nevertheless, the fact that an attacker may have the device in his possession for as long as he likes, and perhaps obtain numerous other samples for testing and practice, means that it is practically impossible to totally eliminate tampering by a sufficiently motivated opponent. Because of this, one of the most important elements in protecting a system is overall system design. In particular, tamper-resistant systems should "fail gracefully" by ensuring that compromise of one device does not compromise the entire system. In this manner, the attacker can be practically restricted to attacks that cost less than the expected return from compromising a single device (plus, perhaps, a little more for kudos). Since the most sophisticated attacks have been estimated to cost several hundred thousand dollars to carry out, carefully designed systems may be invulnerable in practice.

NEW QUESTION 58

- (Topic 1)

Which of the following is an example of discretionary access control?

- A. Identity-based access control
- B. Task-based access control
- C. Role-based access control
- D. Rule-based access control

Answer: A

Explanation:

An identity-based access control is an example of discretionary access control that is based on an individual's identity. Identity-based access control (IBAC) is access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Rule Based Access Control (RuBAC) and Role Based Access Control (RBAC) are examples of non-discretionary access controls.

Rule-based access control is a type of non-discretionary access control because this access is determined by rules and the subject does not decide what those rules will be, the rules are uniformly applied to ALL of the users or subjects.

In general, all access control policies other than DAC are grouped in the category of non-discretionary access control (NDAC). As the name implies, policies in this category have rules that are not established at the discretion of the user. Non-discretionary policies establish controls that cannot be changed by users, but only through administrative action.

Both Role Based Access Control (RBAC) and Rule Based Access Control (RuBAC) fall within Non Discretionary Access Control (NDAC). If it is not DAC or MAC then it is most likely NDAC.

BELOW YOU HAVE A DESCRIPTION OF THE DIFFERENT CATEGORIES:

MAC = Mandatory Access Control

Under a mandatory access control environment, the system or security administrator will define what permissions subjects have on objects. The administrator does not dictate user's access but simply configures the proper level of access as dictated by the Data Owner.

The MAC system will look at the Security Clearance of the subject and compare it with the object sensitivity level or classification level. This is what is called the dominance relationship.

The subject must DOMINATE the object sensitivity level. Which means that the subject must have a security clearance equal or higher than the object he is attempting to access.

MAC also introduces the concept of labels. Every object will have a label attached to them indicating the classification of the object as well as categories that are used to impose the need to know (NTK) principle. Even though a user has a security clearance of Secret it does not mean he would be able to access any Secret documents within the system. He would be allowed to access only Secret document for which he has a Need To Know, formal approval, and object where the user belongs to one of the categories attached to the object.

If there is no clearance and no labels then IT IS NOT Mandatory Access Control.

Many of the other models can mimic MAC but none of them have labels and a dominance relationship so they are NOT in the MAC category.

DAC = Discretionary Access Control

DAC is also known as: Identity Based access control system.

The owner of an object is defined as the person who created the object. As such the owner has the discretion to grant access to other users on the network. Access will be granted based solely on the identity of those users.

Such system is good for low level of security. One of the major problems is the fact that a user who has access to someone else's file can further share the file with other users without the knowledge or permission of the owner of the file. Very quickly this could become the wild wild west as there is no control on the dissemination of the information.

RBAC = Role Based Access Control

RBAC is a form of Non-Discretionary access control.

Role Based access control usually maps directly with the different types of jobs performed by employees within a company.

For example there might be 5 security administrator within your company. Instead of creating each of their profile one by one, you would simply create a role and assign the administrators to the role. Once an administrator has been assigned to a role, he will IMPLICITLY inherit the permissions of that role.

RBAC is great tool for environments where there is a large rotation of employees on a daily basis such as a very large help desk for example.

RBAC or RuBAC = Rule Based Access Control RuBAC is a form of Non-Discretionary access control.

A good example of a Rule Based access control device would be a Firewall. A single set of rules is imposed to all users attempting to connect through the firewall.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the

Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33. and

NISTIR-7316 at <http://csrc.nist.gov/publications/nistir/7316/NISTIR-7316.pdf> and

http://itlaw.wikia.com/wiki/Identity-based_access_control

NEW QUESTION 59

- (Topic 1)

Which of the following is true about Kerberos?

- A. It utilizes public key cryptography.
- B. It encrypts data after a ticket is granted, but passwords are exchanged in plain text.
- C. It depends upon symmetric ciphers.
- D. It is a second party authentication system.

Answer: C

Explanation:

Kerberos depends on secret keys (symmetric ciphers). Kerberos is a third party authentication protocol. It was designed and developed in the mid 1980's by MIT. It is considered open source but is copyrighted and owned by MIT. It relies on the user's secret keys. The password is used to encrypt and decrypt the keys.

The following answers are incorrect:

It utilizes public key cryptography. Is incorrect because Kerberos depends on secret keys (symmetric ciphers).

It encrypts data after a ticket is granted, but passwords are exchanged in plain text. Is incorrect because the passwords are not exchanged but used for encryption and decryption of the keys.

It is a second party authentication system. Is incorrect because Kerberos is a third party authentication system, you authenticate to the third party (Kerberos) and not the system you are accessing.

References:

MIT <http://web.mit.edu/kerberos/>

Wikipedia http://en.wikipedia.org/wiki/Kerberos_%28protocol%29

OIG CBK Access Control (pages 181 - 184) AIOv3 Access Control (pages 151 - 155)

NEW QUESTION 60

- (Topic 1)

Which of the following remote access authentication systems is the most robust?

- A. TACACS+
- B. RADIUS
- C. PAP
- D. TACACS

Answer: A

Explanation:

TACACS+ is a proprietary Cisco enhancement to TACACS and is more robust than RADIUS. PAP is not a remote access authentication system but a remote node security protocol.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 3: Telecommunications and Network Security (page 122).

NEW QUESTION 63

- (Topic 1)

Which of the following would be true about Static password tokens?

- A. The owner identity is authenticated by the token
- B. The owner will never be authenticated by the token.
- C. The owner will authenticate himself to the system.
- D. The token does not authenticates the token owner but the system.

Answer: A

Explanation:

Password Tokens

Tokens are electronic devices or cards that supply a user's password for them. A token system can be used to supply either a static or a dynamic password. There is a big difference between the static and dynamic systems, a static system will normally log a user in but a dynamic system the user will often have to log themselves in.

Static Password Tokens:

The owner identity is authenticated by the token. This is done by the person who issues the token to the owner (normally the employer). The owner of the token is now authenticated by "something you have". The token authenticates the identity of the owner to the information system. An example of this occurring is when an employee swipes his or her smart card over an electronic lock to gain access to a store room.

Synchronous Dynamic Password Tokens:

This system is a lot more complex than the static token password. The synchronous dynamic password tokens generate new passwords at certain time intervals that are synched with the main system. The password is generated on a small device similar to a pager or a calculator that can often be attached to the user's key ring. Each password is only valid for a certain time period, typing in the wrong password in the wrong time period will invalidate the authentication. The time factor can also be the systems downfall. If a clock on the system or the password token device becomes out of synch, a user can have trouble authenticating themselves to the system.

Asynchronous Dynamic Password Tokens:

The clock synching problem is eliminated with asynchronous dynamic password tokens. This system works on the same principle as the synchronous one but it does not have a time frame. A lot of big companies use this system especially for employee's who may work from home on the company's VPN (Virtual private Network).

Challenge Response Tokens:

This is an interesting system. A user will be sent special "challenge" strings at either random or timed intervals. The user inputs this challenge string into their token device and the device will respond by generating a challenge response. The user then types this response into the system and if it is correct they are authenticated.

Reference(s) used for this question: <http://www.informit.com/guides/content.aspx?g=security&seqNum=146>
and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION 65

- (Topic 1)

Which security model ensures that actions that take place at a higher security level do not affect actions that take place at a lower level?

- A. The Bell-LaPadula model
- B. The information flow model
- C. The noninterference model
- D. The Clark-Wilson model

Answer: C

Explanation:

The goal of a noninterference model is to strictly separate differing security levels to assure that higher-level actions do not determine what lower-level users can see. This is in contrast to other security models that control information flows between differing levels of users. By maintaining strict separation of security levels, a noninterference model minimizes leakages that might happen through a covert channel.

The model ensures that any actions that take place at a higher security level do not affect, or interfere with, actions that take place at a lower level.

It is not concerned with the flow of data, but rather with what a subject knows about the state of the system. So if an entity at a higher security level performs an action, it can not change the state for the entity at the lower level.

The model also addresses the inference attack that occurs when some one has access to some type of information and can infer(guess) something that he does not have the clearance level or authority to know.

The following are incorrect answers:

The Bell-LaPadula model is incorrect. The Bell-LaPadula model is concerned only with confidentiality and bases access control decisions on the classification of objects and the clearances of subjects.

The information flow model is incorrect. The information flow models have a similar framework to the Bell-LaPadula model and control how information may flow between objects based on security classes. Information will be allowed to flow only in accordance with the security policy.

The Clark-Wilson model is incorrect. The Clark-Wilson model is concerned with change control and assuring that all modifications to objects preserve integrity by means of well-formed transactions and usage of an access triple (subject - interface - object).

References:

CBK, pp 325 - 326

AIO3, pp. 290 - 291

AIOv4 Security Architecture and Design (page 345)

AIOv5 Security Architecture and Design (pages 347 - 348)

https://en.wikibooks.org/wiki/Security_Architecture_and_Design/Security_Models#Noninterference_Models

NEW QUESTION 66

- (Topic 1)

What physical characteristic does a retinal scan biometric device measure?

- A. The amount of light reaching the retina
- B. The amount of light reflected by the retina
- C. The pattern of light receptors at the back of the eye
- D. The pattern of blood vessels at the back of the eye

Answer: D

Explanation:

The retina, a thin nerve (1/50th of an inch) on the back of the eye, is the part of the eye which senses light and transmits impulses through the optic nerve to the brain - the equivalent of film in a camera. Blood vessels used for biometric identification are located along the neural retina, the outermost of retina's four cell layers.

The following answers are incorrect:

The amount of light reaching the retina The amount of light reaching the retina is not used in the biometric scan of the retina.

The amount of light reflected by the retina The amount of light reflected by the retina is not used in the biometric scan of the retina.

The pattern of light receptors at the back of the eye This is a distractor The following reference(s) were/was used to create this question: Reference: Retina Scan Technology.

ISC2 Official Guide to the CBK, 2007 (Page 161)

NEW QUESTION 67

- (Topic 1)

Which of the following can be defined as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences?

- A. Extensible Authentication Protocol
- B. Challenge Handshake Authentication Protocol
- C. Remote Authentication Dial-In User Service
- D. Multilevel Authentication Protocol.

Answer: A

Explanation:

RFC 2828 (Internet Security Glossary) defines the Extensible Authentication Protocol as a framework that supports multiple, optional authentication mechanisms for PPP, including cleartext passwords, challenge-response, and arbitrary dialog sequences. It is intended for use primarily by a host or router that connects to a PPP network server via switched circuits or dial-up lines. The Remote Authentication Dial-In User Service (RADIUS) is defined as an Internet protocol for carrying dial-in user's authentication information and configuration information between a shared, centralized authentication server and a network access server that needs to authenticate the users of its network access ports. The other option is a distracter.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 69

- (Topic 1)

The controls that usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists are associated with:

- A. Preventive/physical
- B. Detective/technical
- C. Detective/physical
- D. Detective/administrative

Answer: C

Explanation:

Detective/physical controls usually require a human to evaluate the input from sensors or cameras to determine if a real threat exists.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION 71

- (Topic 1)

What is one disadvantage of content-dependent protection of information?

- A. It increases processing overhead.
- B. It requires additional password entry.
- C. It exposes the system to data locking.
- D. It limits the user's individual address space.

Answer: A

Explanation:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 75

- (Topic 1)

What security model implies a central authority that define rules and sometimes global rules, dictating what subjects can have access to what objects?

- A. Flow Model
- B. Discretionary access control
- C. Mandatory access control
- D. Non-discretionary access control

Answer: D

Explanation:

As a security administrator you might configure user profiles so that users cannot change the system's time, alter system configuration files, access a command prompt, or install unapproved applications. This type of access control is referred to as nondiscretionary, meaning that access decisions are not made at the discretion of the user. Nondiscretionary access controls are put into place by an authoritative entity (usually a security administrator) with the goal of protecting the organization's most critical assets.

Non-discretionary access control is when a central authority determines what subjects can have access to what objects based on the organizational security policy. Centralized access control is not an existing security model.

Both, Rule Based Access Control (RuBAC or RBAC) and Role Based Access Controls (RBAC) falls into this category.

Reference(s) used for this question:

Harris, Shon (2012-10-18). CISSP All-in-One Exam Guide, 6th Edition (p. 221). McGraw- Hill. Kindle Edition.

and

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 2: Access control systems (page 33).

NEW QUESTION 79

- (Topic 1)

Which of the following exemplifies proper separation of duties?

- A. Operators are not permitted to modify the system time.
- B. Programmers are permitted to use the system console.
- C. Console operators are permitted to mount tapes and disks.
- D. Tape operators are permitted to use the system console.

Answer: A

Explanation:

This is an example of Separation of Duties because operators are prevented from modifying the system time which could lead to fraud. Tasks of this nature should be performed by system administrators.

AIO defines Separation of Duties as a security principle that splits up a critical task among two or more individuals to ensure that one person cannot complete a risky task by himself.

The following answers are incorrect:

Programmers are permitted to use the system console. Is incorrect because programmers should not be permitted to use the system console, this task should be performed by operators. Allowing programmers access to the system console could allow fraud to occur so this is not an example of Separation of Duties..

Console operators are permitted to mount tapes and disks. Is incorrect because operators should be able to mount tapes and disks so this is not an example of Separation of Duties.

Tape operators are permitted to use the system console. Is incorrect because operators should be able to use the system console so this is not an example of Separation of Duties.

References:

OIG CBK Access Control (page 98 - 101) AIOv3 Access Control (page 182)

NEW QUESTION 84

- (Topic 1)

Which of the following protection devices is used for spot protection within a few inches of the object, rather than for overall room security monitoring?

- A. Wave pattern motion detectors
- B. Capacitance detectors
- C. Field-powered devices
- D. Audio detectors

Answer: B

Explanation:

Capacitance detectors monitor an electrical field surrounding the object being monitored. They are used for spot protection within a few inches of the object, rather than for overall room security monitoring used by wave detectors. Penetration of this field changes the electrical capacitance of the field enough to generate an alarm. Wave pattern motion detectors generate a frequency wave pattern and send an alarm if the pattern is disturbed as it is reflected back to its receiver. Field-

powered devices are a type of personnel access control devices. Audio detectors simply monitor a room for any abnormal sound wave generation and trigger an alarm.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, John Wiley & Sons, 2001, Chapter 10: Physical security (page 344).

NEW QUESTION 89

- (Topic 1)

What mechanism automatically causes an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters?

- A. Central station alarm
- B. Proprietary alarm
- C. A remote station alarm
- D. An auxiliary station alarm

Answer: D

Explanation:

Auxiliary station alarms automatically cause an alarm originating in a data center to be transmitted over the local municipal fire or police alarm circuits for relaying to both the local police/fire station and the appropriate headquarters. They are usually Municipal Fire Alarm Boxes are installed at your business or building, they are wired directly into the fire station.

Central station alarms are operated by private security organizations. It is very similar to a proprietary alarm system (see below). However, the biggest difference is the monitoring and receiving of alarm is done off site at a central location manned by non staff members. It is a third party.

Proprietary alarms are similar to central stations alarms except that monitoring is performed directly on the protected property. This type of alarm is usually use to protect large industrials or commercial buildings. Each of the buildings in the same vicinity has their own alarm system, they are all wired together at a central location within one of the building acting as a common receiving point. This point is usually far away from the other building so it is not under the same danger. It is usually man 24 hours a day by a trained team who knows how to react under different conditions.

A remote station alarm is a direct connection between the signal-initiating device at the protected property and the signal-receiving device located at a remote station, such as the fire station or usually a monitoring service. This is the most popular type of implementation and the owner of the premise must pay a monthly monitoring fee. This is what most people use in their home where they get a company like ADT to receive the alarms on their behalf.

A remote system differs from an auxiliary system in that it does not use the municipal fire or police alarm circuits.

Reference(s) used for this question:

ANDRESS, Mandy, Exam Cram CISSP, Coriolis, 2001, Chapter 11: Physical Security (page 211).

and

Great presentation J.T.A. Stone on SlideShare

NEW QUESTION 92

- (Topic 1)

How can an individual/person best be identified or authenticated to prevent local masquerading attacks?

- A. UserId and password
- B. Smart card and PIN code
- C. Two-factor authentication
- D. Biometrics

Answer: D

Explanation:

The only way to be truly positive in authenticating identity for access is to base the authentication on the physical attributes of the persons themselves (i.e., biometric identification).

Physical attributes cannot be shared, borrowed, or duplicated. They ensure that you do identify the person, however they are not perfect and they would have to be supplemented by another factor.

Some people are getting thrown off by the term Masquerade. In general, a masquerade is a disguise. In terms of communications security issues, a masquerade is a type of attack where the attacker pretends to be an authorized user of a system in order to gain access to it or to gain greater privileges than they are authorized for. A masquerade may be attempted through the use of stolen logon IDs and passwords, through finding security gaps in programs, or through bypassing the authentication mechanism. Spoofing is another term used to describe this type of attack as well.

A UserId only provides for identification.

A password is a weak authentication mechanism since passwords can be disclosed, shared, written down, and more.

A smart card can be stolen and its corresponding PIN code can be guessed by an intruder. A smartcard can be borrowed by a friend of yours and you would have no clue as to who is really logging in using that smart card.

Any form of two-factor authentication not involving biometrics cannot be as reliable as a biometric system to identify the person.

Biometric identifying verification systems control people. If the person with the correct hand, eye, face, signature, or voice is not present, the identification and verification cannot take place and the desired action (i.e., portal passage, data, or resource access) does not occur.

As has been demonstrated many times, adversaries and criminals obtain and successfully use access cards, even those that require the addition of a PIN. This is because these systems control only pieces of plastic (and sometimes information), rather than people. Real asset and resource protection can only be accomplished by people, not cards and information, because unauthorized persons can (and do) obtain the cards and information.

Further, life-cycle costs are significantly reduced because no card or PIN administration system or personnel are required. The authorized person does not lose physical characteristics (i.e., hands, face, eyes, signature, or voice), but cards and PINs are continuously lost, stolen, or forgotten. This is why card access systems require systems and people to administer, control, record, and issue (new) cards and PINs. Moreover, the cards are an expensive and recurring cost.

NOTE FROM CLEMENT:

This question has been generating lots of interest. The keyword in the question is: Individual (the person) and also the authenticated portion as well.

I totally agree with you that Two Factors or Strong Authentication would be the strongest means of authentication. However the question is not asking what is the strongest mean of authentication, it is asking what is the best way to identify the user (individual) behind the technology. When answering questions do not make assumptions to facts not presented in the question or answers.

Nothing can beat Biometrics in such case. You cannot lend your fingerprint and pin to someone else, you cannot borrow one of my eye balls to defeat the Iris or Retina scan. This is why it is the best method to authenticate the user.

I think the reference is playing with semantics and that makes it a bit confusing. I have improved the question to make it a lot clearer and I have also improve the explanations attached with the question.

The reference mentioned above refers to authenticating the identity for access. So the distinction is being made that there is identity and there is authentication. In the case of physical security the enrollment process is where the identity of the user would be validated and then the biometrics features provided by the user would authenticate the user on a one to one matching basis (for authentication) with the reference contained in the database of biometrics templates. In the case

of system access, the user might have to provide a username, a pin, a passphrase, a smart card, and then provide his biometric attributes. Biometric can also be used for Identification purpose where you do a one to many match. You take a facial scan of someone within an airport and you attempt to match it with a large database of known criminal and terrorists. This is how you could use biometric for Identification. There are always THREE means of authentication, they are: Something you know (Type 1) Something you have (Type 2) Something you are (Type 3) Reference(s) used for this question: TIPTON, Harold F. & KRAUSE, Micki, Information Security Management Handbook, 4th edition (volume 1) , 2000, CRC Press, Chapter 1, Biometric Identification (page 7). and Search Security at <http://searchsecurity.techtarget.com/definition/masquerade>

NEW QUESTION 93

- (Topic 1)

What Orange Book security rating is reserved for systems that have been evaluated but fail to meet the criteria and requirements of the higher divisions?

- A. A
- B. D
- C. E
- D. F

Answer: B

Explanation:

D or "minimal protection" is reserved for systems that were evaluated under the TCSEC but did not meet the requirements for a higher trust level. A is incorrect. A or "Verified Protection" is the highest trust level under the TCSEC. E is incorrect. The trust levels are A - D so "E" is not a valid trust level. F is incorrect. The trust levels are A - D so "F" is not a valid trust level. CBK, pp. 329 - 330 AIO3, pp. 302 - 306

NEW QUESTION 97

- (Topic 1)

The number of violations that will be accepted or forgiven before a violation record is produced is called which of the following?

- A. clipping level
- B. acceptance level
- C. forgiveness level
- D. logging level

Answer: A

Explanation:

The correct answer is "clipping level". This is the point at which a system decides to take some sort of action when an action repeats a preset number of times. That action may be to log the activity, lock a user account, temporarily close a port, etc. Example: The most classic example of a clipping level is failed login attempts. If you have a system configured to lock a user's account after three failed login attempts, that is the "clipping level".

The other answers are not correct because:

Acceptance level, forgiveness level, and logging level are nonsensical terms that do not exist (to my knowledge) within network security.

Reference:

Official ISC2 Guide - The term "clipping level" is not in the glossary or index of that book. I cannot find it in the text either. However, I'm quite certain that it would be considered part of the CBK, despite its exclusion from the Official Guide.

All in One Third Edition page: 136 - 137

NEW QUESTION 100

- (Topic 1)

The "vulnerability of a facility" to damage or attack may be assessed by all of the following except:

- A. Inspection
- B. History of losses
- C. Security controls
- D. security budget

Answer: D

Explanation:

Source: The CISSP Examination Textbook- Volume 2: Practice by S. Rao Vallabhaneni.

NEW QUESTION 105

- (Topic 1)

Which of the following best ensures accountability of users for the actions taken within a system or domain?

- A. Identification
- B. Authentication
- C. Authorization
- D. Credentials

Answer: B

Explanation:

Details:

The only way to ensure accountability is if the subject is uniquely identified and authenticated. Identification alone does not provide proof the user is who they claim to be. After showing proper credentials, a user is authorized access to resources.

References:

HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 4: Access Control (page 126).

NEW QUESTION 108

- (Topic 1)

In Synchronous dynamic password tokens:

- A. The token generates a new password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- B. The token generates a new non-unique password value at fixed time intervals (this password could be based on the time of day encrypted with a secret key).
- C. The unique password is not entered into a system or workstation along with an owner's PIN.
- D. The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is invalid and that it was entered during the invalid time window.

Answer: A

Explanation:

Synchronous dynamic password tokens:

- The token generates a new password value at fixed time intervals (this password could be the time of day encrypted with a secret key).
- the unique password is entered into a system or workstation along with an owner's PIN.
- The authentication entity in a system or workstation knows an owner's secret key and PIN, and the entity verifies that the entered password is valid and that it was entered during the valid time window.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 37.

NEW QUESTION 109

- (Topic 1)

Why do buffer overflows happen? What is the main cause?

- A. Because buffers can only hold so much data
- B. Because of improper parameter checking within the application
- C. Because they are an easy weakness to exploit
- D. Because of insufficient system memory

Answer: B

Explanation:

Buffer Overflow attack takes advantage of improper parameter checking within the application. This is the classic form of buffer overflow and occurs because the programmer accepts whatever input the user supplies without checking to make sure that the length of the input is less than the size of the buffer in the program. The buffer overflow problem is one of the oldest and most common problems in software development and programming, dating back to the introduction of interactive computing. It can result when a program fills up the assigned buffer of memory with more data than its buffer can hold. When the program begins to write beyond the end of the buffer, the program's execution path can be changed, or data can be written into areas used by the operating system itself. This can lead to the insertion of malicious code that can be used to gain administrative privileges on the program or system.

As explained by Gaurab, it can become very complex. At the time of input even if you are checking the length of the input, it has to be check against the buffer size. Consider a case where entry point of data is stored in Buffer1 of Application1 and then you copy it to Buffer2 within Application2 later on, if you are just checking the length of data against Buffer1, it will

not ensure that it will not cause a buffer overflow in Buffer2 of Application2.

A bit of reassurance from the ISC2 book about level of Coding Knowledge needed for the exam:

It should be noted that the CISSP is not required to be an expert programmer or know the inner workings of developing application software code, like the FORTRAN programming language, or how to develop Web applet code using Java. It is not even necessary that the CISSP know detailed security-specific coding practices such as the major divisions of buffer overflow exploits or the reason for preferring str(n)cpy to strcpy in the C language (although all such knowledge is, of course, helpful). Because the CISSP may be the person responsible for ensuring that security is included in such developments, the CISSP should know the basic procedures and concepts involved during the design and development of software programming. That is, in order for the CISSP to monitor the software development process and verify that security is included, the CISSP must understand the fundamental concepts of programming developments and the security strengths and weaknesses of various application development processes.

The following are incorrect answers:

"Because buffers can only hold so much data" is incorrect. This is certainly true but is not the best answer because the finite size of the buffer is not the problem -- the problem is that the programmer did not check the size of the input before moving it into the buffer.

"Because they are an easy weakness to exploit" is incorrect. This answer is sometimes true but is not the best answer because the root cause of the buffer overflow is that the programmer did not check the size of the user input.

"Because of insufficient system memory" is incorrect. This is irrelevant to the occurrence of a buffer overflow.

Reference(s) used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 13319-13323). Auerbach Publications. Kindle Edition.

NEW QUESTION 111

- (Topic 1)

Another type of access control is lattice-based access control. In this type of control a lattice model is applied. How is this type of access control concept applied?

- A. The pair of elements is the subject and object, and the subject has an upper bound equal or higher than the upper bound of the object being accessed.
- B. The pair of elements is the subject and object, and the subject has an upper bound lower than the upper bound of the object being accessed.
- C. The pair of elements is the subject and object, and the subject has no special upper or lower bound needed within the lattice.
- D. The pair of elements is the subject and object, and the subject has no access rights in relation to an object.

Answer: A

Explanation:

To apply this concept to access control, the pair of elements is the subject and object, and the subject has to have an upper bound equal or higher than the object

being accessed.

WIKIPEDIA has a great explanation as well:

In computer security, lattice-based access control (LBAC) is a complex access control based on the interaction between any combination of objects (such as resources, computers, and applications) and subjects (such as individuals, groups or organizations). In this type of label-based mandatory access control model, a lattice is used to define the levels of security that an object may have and that a subject may have access to. The subject is only allowed to access an object if the security level of the subject is greater than or equal to that of the object.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 34.
and

http://en.wikipedia.org/wiki/Lattice-based_access_control

NEW QUESTION 116

- (Topic 1)

What is called the act of a user professing an identity to a system, usually in the form of a log-on ID?

- A. Authentication
- B. Identification
- C. Authorization
- D. Confidentiality

Answer: B

Explanation:

Identification is the act of a user professing an identity to a system, usually in the form of a log-on ID to the system.

Identification is nothing more than claiming you are somebody. You identify yourself when you speak to someone on the phone that you don't know, and they ask you who they're speaking to. When you say, ??I'm Jason.??, you've just identified yourself.

In the information security world, this is analogous to entering a username. It's not analogous to entering a password. Entering a password is a method for verifying that you are who you identified yourself as.

NOTE: The word "professing" used above means: "to say that you are, do, or feel something when other people doubt what you say". This is exactly what happens when you provide your identifier (identification), you claim to be someone but the system cannot take your word for it, you must further Authenticate to the system to prove who you claim to be.

The following are incorrect answers:

Authentication: is how one proves that they are who they say they are. When you claim to be Jane Smith by logging into a computer system as ??jsmith??, it's most likely going to ask you for a password. You've claimed to be that person by entering the name into the username field (that's the identification part), but now you have to prove that you are really that person.

Many systems use a password for this, which is based on ??something you know??, i.e. a secret between you and the system.

Another form of authentication is presenting something you have, such as a driver's license, an RSA token, or a smart card.

You can also authenticate via something you are. This is the foundation for biometrics. When you do this, you first identify yourself and then submit a thumb print, a retina scan, or another form of bio-based authentication.

Once you've successfully authenticated, you have now done two things: you've claimed to be someone, and you've proven that you are that person. The only thing that's left is for the system to determine what you're allowed to do.

Authorization: is what takes place after a person has been both identified and authenticated; it's the step determines what a person can then do on the system. An example in people terms would be someone knocking on your door at night. You say, ??Who is it??, and wait for a response. They say, ??It's John.?? in order to identify themselves. You ask them to back up into the light so you can see them through the peephole. They do so, and you authenticate them based on what they look like (biometric). At that point you decide they can come inside the house.

If they had said they were someone you didn't want in your house (identification), and you then verified that it was that person (authentication), the authorization phase would not include access to the inside of the house.

Confidentiality: Is one part of the CIA triad. It prevents sensitive information from reaching the wrong people, while making sure that the right people can in fact get it. A good example is a credit card number while shopping online, the merchant needs it to clear the transaction but you do not want your information exposed over the network, you would use a secure link such as SSL, TLS, or some tunneling tool to protect the information from prying eyes between point A and point B. Data encryption is a common method of ensuring confidentiality.

The other parts of the CIA triad are listed below:

Integrity involves maintaining the consistency, accuracy, and trustworthiness of data over its entire life cycle. Data must not be changed in transit, and steps must be taken to ensure that data cannot be altered by unauthorized people (for example, in a breach of confidentiality). In addition, some means must be in place to detect any changes in data that might occur as a result of non-human-caused events such as an electromagnetic pulse (EMP) or server crash. If an unexpected change occurs, a backup copy must be available to restore the affected data to its correct state.

Availability is best ensured by rigorously maintaining all hardware, performing hardware repairs immediately when needed, providing a certain measure of redundancy and failover, providing adequate communications bandwidth and preventing the occurrence of bottlenecks, implementing emergency backup power systems, keeping current with all necessary system upgrades, and guarding against malicious actions such as denial-of-service (DoS) attacks.

Reference used for this question:

<http://whatis.techtarget.com/definition/Confidentiality-integrity-and-availability-CIA> <http://www.danielmiessler.com/blog/security-identification-authentication-and-authorization> <http://www.merriam-webster.com/dictionary/profess>

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 36.

NEW QUESTION 120

- (Topic 1)

What is the Biba security model concerned with?

- A. Confidentiality
- B. Reliability
- C. Availability
- D. Integrity

Answer: D

Explanation:

The Biba security model addresses the integrity of data being threatened when subjects at lower security levels are able to write to objects at higher security levels and when subjects can read data at lower levels.

Source: HARRIS, Shon, All-In-One CISSP Certification Exam Guide, McGraw-Hill/Osborne, 2002, Chapter 5: Security Models and Architecture (Page 244).

NEW QUESTION 125

- (Topic 1)

There are parallels between the trust models in Kerberos and Public Key Infrastructure (PKI). When we compare them side by side, Kerberos tickets correspond most closely to which of the following?

- A. public keys
- B. private keys
- C. public-key certificates
- D. private-key certificates

Answer: C

Explanation:

A Kerberos ticket is issued by a trusted third party. It is an encrypted data structure that includes the service encryption key. In that sense it is similar to a public-key certificate. However, the ticket is not the key.

The following answers are incorrect:

public keys. Kerberos tickets are not shared out publicly, so they are not like a PKI public key.

private keys. Although a Kerberos ticket is not shared publicly, it is not a private key. Private keys are associated with Asymmetric crypto system which is not used by Kerberos. Kerberos uses only the Symmetric crypto system.

private key certificates. This is a detractor. There is no such thing as a private key certificate.

NEW QUESTION 130

- (Topic 1)

In response to Access-request from a client such as a Network Access Server (NAS), which of the following is not one of the response from a RADIUS Server?

- A. Access-Accept
- B. Access-Reject
- C. Access-Granted
- D. Access-Challenge

Answer: C

Explanation:

In response to an access-request from a client, a RADIUS server returns one of three authentication responses: access-accept, access-reject, or access-challenge, the latter being a request for additional authentication information such as a one-time password from a token or a callback identifier.

Source: TIPTON, Harold F. & KRAUSE, MICKI, Information Security Management Handbook, 4th Edition, Volume 2, 2001, CRC Press, NY, page 36.

NEW QUESTION 132

- (Topic 1)

Which access control model would a lattice-based access control model be an example of?

- A. Mandatory access control.
- B. Discretionary access control.
- C. Non-discretionary access control.
- D. Rule-based access control.

Answer: A

Explanation:

In a lattice model, there are pairs of elements that have the least upper bound of values and greatest lower bound of values. In a Mandatory Access Control (MAC) model, users and data owners do not have as much freedom to determine who can access files.

TIPS FROM CLEMENT

Mandatory Access Control is in place whenever you have permissions that are being imposed on the subject and the subject cannot arbitrarily change them. When the subject/owner of the file can change permissions at will, it is discretionary access control.

Here is a breakdown largely based on explanations provided by Doug Landoll. I am reproducing below using my own word and not exactly how Doug explained it:

FIRST: The Lattice

A lattice is simply an access control tool usually used to implement Mandatory Access Control (MAC) and it could also be used to implement RBAC but this is not as common. The lattice model can be used for Integrity level or file permissions as well. The lattice has a least upper bound and greatest lower bound. It makes use of pair of elements such as the subject security clearance pairing with the object sensitivity label.

SECOND: DAC (Discretionary Access Control)

Let's get into Discretionary Access Control: It is an access control method where the owner (read the creator of the object) will decide who has access at his own discretion. As we all know, users are sometimes insane. They will share their files with other users based on their identity but nothing prevent the user from further sharing it with other users on the network. Very quickly you loose control on the flow of information and who has access to what. It is used in small and friendly environment where a low level of security is all that is required.

THIRD: MAC (Mandatory Access Control)

All of the following are forms of Mandatory Access Control: Mandatory Access control (MAC) (Implemented using the lattice)

You must remember that MAC makes use of Security Clearance for the subject and also Labels will be assigned to the objects. The clearance of the Subject must dominate (be equal or higher) the clearance of the Object being accessed. The label attached to the object will indicate the sensitivity level and the categories the object belongs to. The categories are used to implement the Need to Know.

All of the following are forms of Non Discretionary Access Control:

Role Based Access Control (RBAC)

Rule Based Access Control (Think Firewall in this case)

The official ISC2 book says that RBAC (synonymous with Non Discretionary Access Control) is a form of DAC but they are simply wrong. RBAC is a form of Non Discretionary Access Control. Non Discretionary DOES NOT equal mandatory access control as there is no labels and clearance involved.

I hope this clarifies the whole drama related to what is what in the world of access control. In the same line of taught, you should be familiar with the difference between Explicit

permission (the user has his own profile) versus Implicit (the user inherit permissions by being a member of a role for example).

The following answers are incorrect:

Discretionary access control. Is incorrect because in a Discretionary Access Control (DAC) model, access is restricted based on the authorization granted to the

users. It is identity based access control only. It does not make use of a lattice.

Non-discretionary access control. Is incorrect because Non-discretionary Access Control (NDAC) uses the role-based access control method to determine access rights and permissions. It is often times used as a synonym to RBAC which is Role Based Access Control. The user inherit permission from the role when they are assigned into the role. This type of access could make use of a lattice but could also be implemented without the use of a lattice in some case. Mandatory Access Control was a better choice than this one, but RBAC could also make use of a lattice. The BEST answer was MAC.

Rule-based access control. Is incorrect because it is an example of a Non-discretionary Access Control (NDAC) access control mode. You have rules that are globally applied to all users. There is no such thing as a lattice being use in Rule-Based Access Control.

References:

AIOv3 Access Control (pages 161 - 168)

AIOv3 Security Models and Architecture (pages 291 - 293)

NEW QUESTION 135

- (Topic 1)

Which access model is most appropriate for companies with a high employee turnover?

- A. Role-based access control
- B. Mandatory access control
- C. Lattice-based access control
- D. Discretionary access control

Answer: A

Explanation:

The underlying problem for a company with a lot of turnover is assuring that new employees are assigned the correct access permissions and that those permissions are removed when they leave the company.

Selecting the best answer requires one to think about the access control options in the context of a company with a lot of flux in the employee population. RBAC simplifies the task of assigning permissions because the permissions are assigned to roles which do not change based on who belongs to them. As employees join the company, it is simply a matter of assigning them to the appropriate roles and their permissions derive from their assigned role. They will implicitly inherit the permissions of the role or roles they have been assigned to. When they leave the company or change jobs, their role assignment is revoked/changed appropriately.

Mandatory access control is incorrect. While controlling access based on the clearance level of employees and the sensitivity of objects is a better choice than some of the other incorrect answers, it is not the best choice when RBAC is an option and you are looking for the best solution for a high number of employees constantly leaving or joining the company.

Lattice-based access control is incorrect. The lattice is really a mathematical concept that is used in formally modeling information flow (Bell-Lapadula, Biba, etc). In the context of the question, an abstract model of information flow is not an appropriate choice. CBK, pp. 324- 325.

Discretionary access control is incorrect. When an employee joins or leaves the company, the object owner must grant or revoke access for that employee on all the objects they own. Problems would also arise when the owner of an object leaves the company. The complexity of assuring that the permissions are added and removed correctly makes this the least desirable solution in this situation.

References

All in One, third edition page 165

RBAC is discussed on pp. 189 through 191 of the ISC(2) guide.

NEW QUESTION 136

- (Topic 1)

Considerations of privacy, invasiveness, and psychological and physical comfort when using the system are important elements for which of the following?

- A. Accountability of biometrics systems
- B. Acceptability of biometrics systems
- C. Availability of biometrics systems
- D. Adaptability of biometrics systems

Answer: B

Explanation:

Acceptability refers to considerations of privacy, invasiveness, and psychological and physical comfort when using the system.

Source: KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 39.

NEW QUESTION 138

- (Topic 1)

Which of the following security controls might force an operator into collusion with personnel assigned organizationally within a different function in order to gain access to unauthorized data?

- A. Limiting the local access of operations personnel
- B. Job rotation of operations personnel
- C. Management monitoring of audit logs
- D. Enforcing regular password changes

Answer: A

Explanation:

The questions specifically said: "within a different function" which eliminate Job Rotation as a choice.

Management monitoring of audit logs is a detective control and it would not prevent collusion.

Changing passwords regularly would not prevent such attack.

This question validates if you understand the concept of separation of duties and least privilege. By having operators that have only the minimum access level they need and only what they need to do their duties within a company, the operations personnel would be forced to use collusion to defeat those security mechanism.

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 143

- (Topic 1)

The Computer Security Policy Model the Orange Book is based on is which of the following?

- A. Bell-LaPadula
- B. Data Encryption Standard
- C. Kerberos
- D. Tempest

Answer: A

Explanation:

The Computer Security Policy Model Orange Book is based is the Bell- LaPadula Model. Orange Book Glossary.

The Data Encryption Standard (DES) is a cryptographic algorithm. National Information Security Glossary.

TEMPEST is related to limiting the electromagnetic emanations from electronic equipment. Reference: U.S. Department of Defense, Trusted Computer System Evaluation Criteria (Orange Book), DOD 5200.28-STD. December 1985 (also available here).

NEW QUESTION 145

- (Topic 1)

An access system that grants users only those rights necessary for them to perform their work is operating on which security principle?

- A. Discretionary Access
- B. Least Privilege
- C. Mandatory Access
- D. Separation of Duties

Answer: B

Explanation:

Source: TIPTON, Hal, (ISC)2, Introduction to the CISSP Exam presentation.

NEW QUESTION 149

- (Topic 1)

Which of the following is related to physical security and is not considered a technical control?

- A. Access control Mechanisms
- B. Intrusion Detection Systems
- C. Firewalls
- D. Locks

Answer: D

Explanation:

All of the above are considered technical controls except for locks, which are physical controls.

Administrative, Technical, and Physical Security Controls

Administrative security controls are primarily policies and procedures put into place to define and guide employee actions in dealing with the organization's sensitive information. For example, policy might dictate (and procedures indicate how) that human resources conduct background checks on employees with access to sensitive information. Requiring that information be classified and the process to classify and review information classifications is another example of an administrative control. The organization security awareness program is an administrative control used to make employees cognizant of their security roles and responsibilities. Note that administrative security controls in the form of a policy can be enforced or verified with technical or physical security controls. For instance,

security policy may state that computers without antivirus software cannot connect to the network, but a technical control, such as network access control software, will check for antivirus software when a computer tries to attach to the network.

Technical security controls (also called logical controls) are devices, processes, protocols, and other measures used to protect the C.I.A. of sensitive information. Examples include logical access systems, encryption systems, antivirus systems, firewalls, and intrusion detection systems.

Physical security controls are devices and means to control physical access to sensitive information and to protect the availability of the information. Examples are physical access systems (fences, mantraps, guards), physical intrusion detection systems (motion detector, alarm system), and physical protection systems (sprinklers, backup generator). Administrative and technical controls depend on proper physical security controls being in place. An administrative policy allowing only authorized employees access to the data center do little good without some kind of physical access control.

From the GIAC.ORG website

NEW QUESTION 151

- (Topic 1)

Password management falls into which control category?

- A. Compensating
- B. Detective
- C. Preventive
- D. Technical

Answer: C

Explanation:

Password management is an example of preventive control. Proper passwords prevent unauthorized users from accessing a system.

There are literally hundreds of different access approaches, control methods, and technologies, both in the physical world and in the virtual electronic world. Each method addresses a different type of access control or a specific access need.

For example, access control solutions may incorporate identification and authentication mechanisms, filters, rules, rights, logging and monitoring, policy, and a plethora of other

controls. However, despite the diversity of access control methods, all access control systems can be categorized into seven primary categories.

The seven main categories of access control are:

1. Directive: Controls designed to specify acceptable rules of behavior within an organization
2. Deterrent: Controls designed to discourage people from violating security directives

3. Preventive: Controls implemented to prevent a security incident or information breach
4. Compensating: Controls implemented to substitute for the loss of primary controls and mitigate risk down to an acceptable level
5. Detective: Controls designed to signal a warning when a security control has been breached
6. Corrective: Controls implemented to remedy circumstance, mitigate damage, or restore controls
7. Recovery: Controls implemented to restore conditions to normal after a security incident

Reference(s) used for this question:
Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 1156-1176). Auerbach Publications. Kindle Edition.

NEW QUESTION 153

- (Topic 1)

An attack initiated by an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization is known as a(n):

- A. active attack
- B. outside attack
- C. inside attack
- D. passive attack

Answer: C

Explanation:

An inside attack is an attack initiated by an entity inside the security perimeter, an entity that is authorized to access system resources but uses them in a way not approved by those who granted the authorization whereas an outside attack is initiated from outside the perimeter, by an unauthorized or illegitimate user of the system. An active attack attempts to alter system resources to affect their operation and a passive attack attempts to learn or make use of the information from the system but does not affect system resources.

Source: SHIREY, Robert W., RFC2828: Internet Security Glossary, may 2000.

NEW QUESTION 157

- (Topic 1)

Which of the following are not Remote Access concerns?

- A. Justification for remote access
- B. Auditing of activities
- C. Regular review of access privileges
- D. Access badges

Answer: D

Explanation:

Access badges are more relevant to physical security rather than remote access.

"Justification for remote access" is incorrect. Justification for remote access is a relevant concern.

"Auditing of activities" is incorrect. Auditing of activities is an important aspect to assure that malicious or unauthorized activities are not occurring.

"Regular review of access privileges" is incorrect. Regular review of remote access privileges is an important management responsibility.

References:

AIO3, pp. 547 - 548

NEW QUESTION 162

- (Topic 1)

Which of the following classes is the first level (lower) defined in the TCSEC (Orange Book) as mandatory protection?

- A. B
- B. A
- C. C
- D. D

Answer: A

Explanation:

B level is the first Mandatory Access Control Level.

First published in 1983 and updated in 1985, the TCSEC, frequently referred to as the Orange Book, was a United States Government Department of Defense (DoD) standard that sets basic standards for the implementation of security protections in computing systems. Primarily intended to help the DoD find products that met those basic standards, TCSEC was used to evaluate, classify, and select computer systems being considered for the processing, storage, and retrieval of sensitive or classified information on military and government systems. As such, it was strongly focused on enforcing confidentiality with no focus on other aspects of security such as integrity or availability. Although it has since been superseded by the common criteria, it influenced the development of other product evaluation criteria, and some of its basic approach and terminology continues to be used.

Reference used for this question:

Hernandez CISSP, Steven (2012-12-21). Official (ISC)2 Guide to the CISSP CBK, Third Edition ((ISC)2 Press) (Kindle Locations 17920-17926). Auerbach Publications. Kindle Edition.

and

THE source for all TCSEC "level" questions: <http://csrc.nist.gov/publications/secpubs/rainbow/std001.txt> (paragraph 3 for this one)

NEW QUESTION 166

- (Topic 1)

In Discretionary Access Control the subject has authority, within certain limitations,

- A. but he is not permitted to specify what objects can be accessible and so we need to get an independent third party to specify what objects can be accessible.
- B. to specify what objects can be accessible.
- C. to specify on a aggregate basis without understanding what objects can be accessible.
- D. to specify in full detail what objects can be accessible.

Answer: B

Explanation:

With Discretionary Access Control, the subject has authority, within certain limitations, to specify what objects can be accessible. For example, access control lists can be used. This type of access control is used in local, dynamic situations where the subjects must have the discretion to specify what resources certain users are permitted to access. When a user, within certain limitations, has the right to alter the access control to certain objects, this is termed as user-directed discretionary access control. In some instances, a hybrid approach is used, which combines the features of user-based and identity-based discretionary access control.

References:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 33. and HARRIS, Shon, All-In-One CISSP Certification Exam Guide 5th Edition, McGraw- Hill/Osborne, 2010, Chapter 4: Access Control (page 210-211).

NEW QUESTION 171

- (Topic 1)

Which of the following questions is less likely to help in assessing physical and environmental protection?

- A. Are entry codes changed periodically?
- B. Are appropriate fire suppression and prevention devices installed and working?
- C. Are there processes to ensure that unauthorized individuals cannot read, copy, alter, or steal printed or electronic information?
- D. Is physical access to data transmission lines controlled?

Answer: C

Explanation:

Physical security and environmental security are part of operational controls, and are measures taken to protect systems, buildings, and related supporting infrastructures against threats associated with their physical environment. All the questions above are useful in assessing physical and environmental protection except for the one regarding processes that ensuring that unauthorized individuals cannot access information, which is more a production control.

Source: SWANSON, Marianne, NIST Special Publication 800-26, Security Self- Assessment Guide for Information Technology Systems, November 2001 (Pages A-21 to A-24).

NEW QUESTION 173

- (Topic 1)

Which of the following is addressed by Kerberos?

- A. Confidentiality and Integrity
- B. Authentication and Availability
- C. Validation and Integrity
- D. Auditability and Integrity

Answer: A

Explanation:

Kerberos addresses the confidentiality and integrity of information. It also addresses primarily authentication but does not directly address availability.

Reference(s) used for this question:

KRUTZ, Ronald L. & VINES, Russel D., The CISSP Prep Guide: Mastering the Ten Domains of Computer Security, 2001, John Wiley & Sons, Page 42. and <https://www.ietf.org/rfc/rfc4120.txt> and <http://learn-networking.com/network-security/how-kerberos-authentication-works>

NEW QUESTION 177

.....

Thank You for Trying Our Product

We offer two products:

1st - We have Practice Tests Software with Actual Exam Questions

2nd - Questions and Answers in PDF Format

SSCP Practice Exam Features:

- * SSCP Questions and Answers Updated Frequently
- * SSCP Practice Questions Verified by Expert Senior Certified Staff
- * SSCP Most Realistic Questions that Guarantee you a Pass on Your First Try
- * SSCP Practice Test Questions in Multiple Choice Formats and Updates for 1 Year

100% Actual & Verified — Instant Download, Please Click
[Order The SSCP Practice Test Here](https://www.surepassexam.com/SSCP-exam-dumps.html)